IN THE CLAIMS:

Please amend the following claims:

1. (Amended) A cryptographic communication system comprising:

a plurality of user communication interfaces, each of said communication [interface] interfaces including:

a data receiver;

a string generator;

a data processor connected to said string generator; and

a memory connected to said string generator, said memory having stored a seed value;

a master station, said master station including:

a data transmitter

a second string generator;

a second data processor connected to said second string generator; and a second memory connected to said second string generator, said second memory having stored said seed value[,].

3. (Amended) The cryptographic communication system according to claim 1,

wherein each of said plurality of user communication [interface] interfaces further includes a key block formation device, and

wherein said master station further includes a second key block formation device.

4. (Amended) The cryptographic communication system according to claim 1, wherein each of said plurality of user communication [interface] interfaces is connected to said master station through a communication network.

A3 cont'd

5. (Amended) The cryptographic communication system according to claim 1, wherein each of said plurality of user communication [interface] interfaces communicates with the master station via a wireless network.

7. (Amended) The cryptographic communication system according to claim 6,

wherein said second memory of said master station includes a plurality of seed values, and

A4

wherein each of said seed values stored in said second memory correspond to a value stored by the memory of one of said plurality of said user communication [interface] interfaces.

8. (Amended) The cryptographic communication system according to claim 1,

wherein said second memory of said master station stores a user address value for each of said plurality of user communication [interface] interfaces.

9. (Amended) The cryptographic communication system according to claim 8, wherein each of the seed values stored in said second memory is referenced to [by] the user address value corresponding to the user communication interface in which the seed value is stored.

10. (Amended) The cryptographic communication system according to claim 1,

wherein said second memory of said master station stores a user identification for each of said plurality of user communication [interface] interfaces.

11. (Amended) The cryptographic communication system according to claim 10, wherein each of the seed values stored in said second memory is referenced to [by] the user identification corresponding to the user communication interface in which the seed value is stored.

12. (Amended) The cryptographic communication system according to claim 1,

wherein each of said plurality of user communication [interface] interfaces further includes a data decryptor, and

wherein said master station further includes a master data encryptor.

14. (Amended) The cryptographic communication system according to claim 1,

A5

wherein the memory of at least one of said user communication [interface] interfaces includes a configurable common seed value, and

wherein the master memory of the master station includes said configurable common seed value.

48. (Amended) A computer readable medium including executable instructions for causing a processor to perform a method of cryptographic communication, said method comprising the following steps:

A6

generating data strings;

forming an encryption key using said data strings;

encrypting [programming] a signal using said encryption key; and

transmitting the [programming] encrypted signal.

A7

50. (Amended) The computer readable medium of claim 48, wherein said method further comprises the step of determining whether to encrypt the [programming] signal prior to transmitting said signal.